А. М. Ц ы б у л и н (Волгоград, ВолГУ). **Многоагентная модель для исследования противоборства службы безопасности и ассоциации злоумышленников.**

Для исследования противоборства службы безопасности информационной системы (ИС) и ассоциации злоумышленников разработана многоагентная модель. Она включает в себя множества агентов-нарушителей и агентов системы безопасности, которые являются активными агентами, и агента ИС — пассивный агент. Активные агенты способны выбирать наиболее рациональные стратегии защиты и нападения в зависимости от располагаемых знаний об ИС и обучаться в процессе выполнения своих действий. Формально агент описывается кортежем $A = \langle \text{К}, \text{В}, \text{Т}, \text{З}, \text{И}, \text{С}, \text{П} \rangle$, где К — класс агента; В — вид агента; Т — время жизни агента; З — совокупность знаний; И — множество инструментальных средств; С — множество стратегий; П — пользовательский идентификатор. Выделяются следующие классы агентов: агенты службы защиты информации ($\text{А}_{\text{сб}}$), агенты ИС ($\text{А}_{\text{ис}}$), агенты–злоумышленники ($\text{А}_{\text{зл}}$). Полный набор знаний $\text{З} = \{\text{З}_1, \ldots, \text{З}_n\}$ об уязвимостях аппаратных и программных средств ИС, полученный с применением всех возможных инструментов, и онтологию уязвимостей агент ИС размещает в своей базе знаний. На основе этих знаний агент ИС синтезирует дерево уязвимостей ИС, $G_{\text{ИС}}$ [1], используя алгоритм на базе аппарата марковских ветвящихся процессов. Агент службы безопасности, исходя из реализуемой стратегии, конкретных возможностей и инструментария (средств обнаружения уязвимостей и средств защиты информации), и на основе своей базы знаний синтезирует дерево уязвимостей ИС, $G_{\text{СБ}}$. Аналогично, агент–злоумышленник синтезирует дерево уязвимостей ИС, $G_{\text{ЗЛ}}$.

Каждому ребру дерева приписывается кортеж $E = \langle P, T, R, L, D, F \rangle$, где $\text{P} = \max_i P_i$ — максимальная вероятность успешной реализации атаки (защиты) уязвимости; P_i $(i = 1, \ldots, N)$ — вероятность реализации данной уязвимости при использовании i-го инструмента атаки (защиты), где N — количество доступных инструментов; T — время реализации атаки с использованием данной уязвимости; R — риск, $R = Y\,P$, где Y — ущерб, который наносится реализацией данной атаки ИС; L — уровень данной уязвимости в классификации модели OSI; D — флаг, помечающий соответствующую уязвимость как детектируемую системой диагностики атак; F — флаг, содержащий булевы пометки о факте реализации данной уязвимости.

После того как построены деревья ИС $G_{\text{ИС}} = (E^{\text{ИС}}, V^{\text{ИС}})$ и службы безопасности $G_{\text{СБ}} = (E^{\text{СБ}}, V^{\text{СБ}})$, с помощью наложения этих двух деревьев строится дерево политики безопасности $G_{\text{ПБ}} = (E^{\text{ПБ}}, V^{\text{ПБ}})$, где $V^{\text{ПБ}} = V^{\text{ИС}}$,

$$E_i^{\text{ПБ}} = \begin{cases} E_i^{\text{СБ}}, & \text{если } E_i^{\text{ИС}} \in E^{\text{СБ}}, \\ E_i^{\text{ИС}}, & \text{если } E_i^{\text{ИС}} \notin E^{\text{СБ}}, \end{cases} \quad i = 1, \ldots, K,$$

где K — количество ребер в дереве $G_{\text{ис}}$.

В соответствии с выбранной стратегией агент $\text{А}_{\text{зл}}$ на основе своего синтезированного дерева уязвимостей выбирает маршрут достижения цели. При переходе по соответствующему ребру выбранного маршрута атрибуты ребра (в частности, вероятность и время перехода) соответствуют атрибутам в дереве политики безопасности построенного службой безопасности.

Данная модель позволяет исследовать достаточность политики безопасности информационной системы для отражения атак ассоциации злоумышленников. Программа многоагентной модели реализована на языке С-Шарп и имеет удобный пользовательский интерфейс. В докладе приведены результаты исследований, полученных на модели.

СПИСОК ЛИТЕРАТУРЫ

1. *Цыбулин А. М.*, *Шипилева А. В.* Математическая модель дерева атак на автоматизированную систему. — Обозрение прикл. и промышл. матем., 2008, т. 15, в. 1, с. 183–184.